

Notice of Allowability	Application No.	Applicant(s)
	10/019,012	BRISCOE, ROBERT JOHN
	Examiner	Art Unit
	Ronald Baum	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTO-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. This communication is responsive to 9/18/06.
2. The allowed claim(s) is/are 1-24.
3. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All
 - b) Some*
 - c) None
 of the:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) hereto or 2) to Paper No./Mail Date _____.
 - (b) including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. Notice of References Cited (PTO-892)
2. Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. Notice of Informal Patent Application
6. Interview Summary (PTO-413),
Paper No./Mail Date _____.
7. Examiner's Amendment/Comment
8. Examiner's Statement of Reasons for Allowance
9. Other _____.

NASSER MOAZZAMI
 SUPERVISORY PATENT EXAMINER
 TECHNOLOGY CENTER 2100

DETAILED ACTION

Examiner's Statement of Reasons for Allowance

1. Claims 1-27 are allowed over prior art.
2. This action is in reply to applicant's correspondence of 16 September 2006.
3. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.
4. As per claims 1,11,12,18,19 and 22 generally, prior art of record, Kambayashi et al, U.S. Patent 6,477,649 B2, fails to teach alone, or in combination, other than via hindsight, at the time of the invention, the features as discussed and remarked upon in the response of 9/16/2006 to office action of 5/16/2006.

Specifically, (as per claim 1, for example) prior art dealing with secured/protected (i.e., DRM) content via various cryptographic functions (i.e., encryption/decryption) in general, and video on demand (Vod) insofar as watermarking/encrypted distortion of content and subsequent recovery via decryption, etc., more particularly, is generally known to exist per se, (i.e., Griwodz, C., et al, 'Protecting VoD the Easier Way', ACM, 1998, pages 21-28, <http://delivery.acm.org/10.1145/300000/290751/p21-griwodz.pdf?key1=290751&key2=3917124611&coll=GUIDE&dl=GUIDE&CFID=6825858&CFTOKEN=77234375>, whereas the use of the content multicast in partially corrupted or encrypted form to be subsequently recovered via unicast transfer of encrypted non-corrupted partial content of which predetermined seed components are used to decrypt (via key generation from the seed(s)) said encrypted non-corrupted partial content). Nowhere in the prior art is found collectively the *italicized* claim elements (i.e., the use of a subset of the keys generated and the subset bounded as a function of the predetermined/pre-established seed(s) at the client terminal, so as to allow appropriate distributed content recovery via the use of the subset of keys as a function of the seed(s) so determining the subset via position within the entire

key space), at the *time of the invention*; serving to patently distinguish the invention from said prior art;

“1. A method of distributing data comprising:

(a) *encrypting a plurality of data units each with
a different one of a first sequence of keys;*

(b) communicating encrypted data units to
a plurality of user terminals;

(c) *communicating at least one seed value to
a user terminal;*

(d) *generating from the seed value or values
a second sequence of keys greater in number than
the number of seed values communicated to the user terminal; and*

(e) decrypting data units at the user terminal using
said second sequence of keys,
characterized
*in that in step (d) a sequence of keys constituting
an arbitrarily doubly bounded portion of
the sequence of keys of step (a) is generated, and
in that the position in sequence of
the lower and upper bounds of the said portion are*

determined by the at least one seed value

communicated in step (c)."

5. Dependent claims 2-10,13-17,20,21,23 and 24 are allowable by virtue of their dependencies.

Conclusion

6. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2000

11/27/06

